



IMPACT OF QUANTUM COMPUTING ON TRADITIONAL CRYPTOGRAPHY: AN ANALYTICAL STUDY OF THE LIMITATIONS AND ADVANTAGES OF QUANTUM CRYPTOGRAPHY

Puranjay Haldankar

Research Scholars Program, Harvard Student Agencies, In collaboration with Learn with Leaders

ABSTRACT

The development in the field of quantum computing presents many opportunities as well as challenges in the field of cyber security and cryptography. The emergence of quantum computing will result in the development of systems capable of running advanced algorithms such as Shor's algorithm, which completely undermines the security of traditional cryptography (RSA and ECC). This study delves into the advantages as well as limitations of possible solutions such as post-quantum cryptography (PQC) and quantum key distribution (QKD) in providing robust security in the era of quantum computing and provides background on 'qubits', superposition, and entanglement, which are aspects responsible for making quantum computing powerful. The study also provides suggestions regarding the future development of quantum computing, quantum cryptography, and quantum technologies to support a natural and seamless transition to quantum cryptography as humanity progresses toward a quantum society. The research also highlights the current limitations and constraints of quantum cryptography that are necessary to overcome in the future.

KEYWORDS: Quantum Computing, Cryptography Vulnerabilities, Post-Quantum Cryptography (PQC), Quantum Key Distribution (QKD), Cybersecurity Advancements, Shor's Algorithm

INTRODUCTION

Cybersecurity is a domain within computing that has undergone rapid evolution and significant advancements over the past three decades. In the contemporary landscape, our reliance on digital platforms for communication, commerce, and information storage has grown exponentially (Ajala, 2024). The significant advancements in the field of cybersecurity act as a double-edged sword, as these advancements not only make systems more secure but also provide greater quality resources for cyber threats to utilize. The rapid development in the field of quantum computing resulting in greater computing capabilities threatens the fundamental security of existing cryptography algorithms.

Quantum computing is based on fundamental principles of quantum mechanics and promises to revolutionize the computational capabilities of the universe (Cherbal, 2023). Traditionally, processed data called information is stored in computers in the form of bits (Binary Digits) i.e., 0 and 1 (Sihare, 2024). However, quantum computing and quantum computers utilize a 'qubit' as the basic unit of information. Qubits can exist simultaneously as '0' and '1'. It encodes two complex numbers at once. A quantum computer promises to be immensely powerful because it can be in multiple states at once (Sihare, 2024). The emergence of quantum computing has significant implications for cybersecurity, especially in cryptography. Traditional cryptography techniques, such as RSA and ECC, rely on the difficulty of factoring large numbers for security. However, quantum computers can efficiently factor large numbers using algorithms like Shor's algorithm, which presents a substantial risk to the security of encrypted data. Essentially, all current cryptography algorithms will

fall short of defending against quantum threats simply due to the sheer power quantum computers will possess, as current cryptography algorithms leverage the use of large integers as their security keys, which quantum computers will easily be able to factor into their components. Hence, new quantum encryption techniques such as post-quantum cryptography (PQC) (Bavdekar, 2024) and quantum key distribution (QKD) (Ahilan, 2024) have been developed to protect against quantum threats (Fatima, 2024). The problems arise from the fact that current cryptography methods will not be viable to safeguard digital systems against quantum threats in a future where quantum computing is inevitable. Therefore, by means of this research paper, the vulnerabilities of current cryptography methods such as RSA and ECC to the sheer power of quantum computers have been thoroughly investigated while exploring the requirements, limitations, and advantages of subsequent cryptography methods such as QKD in the quantum era.

LITERATURE REVIEW

R. Azari's and A. N. Salsabila's study, titled Analyzing the Impact of Quantum Computing on Current Encryption Techniques (2024), presents a detailed research methodology to test out the kind of impact increasing the number of qubits, the basic unit of a quantum computer, has on traditional asymmetric-key cryptography algorithms such as RSA and AES using various simulation models, portraying a rather analytical approach to prove the futility of traditional cryptography. The findings of this study show that quantum computing power, which is directly proportional to the number of qubits used, has a negative relationship with the time taken to crack RSA and AES. In the simulations used, the time taken to crack RSA

decreases from approximately 10 hours to 30 minutes when the number of qubits is increased from 30 to 50. Similarly, the time taken to crack AES decreases by half when the number of qubits is doubled. Azari & Salsabila (2024) concluded this study by acknowledging that society is progressing towards the quantum era, and hence developments in the field of cryptography are essential for robust security in the future.

Similarly, the research article published by E. Fatima, A. M. Akthar, and M. Arslan, titled *Evaluating Quantum Cybersecurity: A Comparative Study of Advanced Encryption Methods* (2024), provides a surface-level analysis of the sheer potential of quantum computing and emphasizes the futility of traditional cryptography against quantum computers in the future. Following a cause-and-effect structure, the research article then discusses why QKD and PQC would be adequate solutions to this inevitable problem, emphasizing not only the advantages but also the limitations of the application of QKD and PQC. Other studies, such as Ajala's study, titled *Exploring and Reviewing the Potential of Quantum Computing in Enhancing Cybersecurity Encryption Methods* (2024), and Dervisevik's study, titled *Quantum Key Distribution Networks—Key Management: A Survey* (2024), also acknowledge QKD's usefulness and security against the sheer power of quantum computing but simultaneously also emphasize its impracticality and limitations in today's time. Therefore, by reviewing this literature, it is justified to conclude that traditional cryptography will turn futile in a future where quantum computing is inevitable and to conclude that although quantum cryptography such as PQC and QKD show promising results in providing robust cryptography and digital security in the future, it is a sincere requirement to overcome the technological constraints and limitations with the application of quantum cryptography.

METHODOLOGY

This paper employs a secondary qualitative methodology to analyze the impact of quantum computing on traditional cryptography. Existing academic literature, simulation results, and case studies were reviewed to explore the vulnerabilities of RSA and ECC to quantum algorithms like Shor's algorithm. Additionally, the research assesses potential alternatives, such as Post-Quantum Cryptography (PQC) and Quantum Key Distribution (QKD), to address emerging threats.

This approach was chosen to synthesize comprehensive insights from established studies without requiring primary data collection, enabling a detailed examination of theoretical and practical advancements in quantum cryptography. However, the reliance on secondary data introduces limitations, such as potential biases within sources and the absence of real-world experimental validations of quantum-resistant solutions. Despite these constraints, the methodology is suitable for providing a thorough foundation for understanding quantum computing's implications on cybersecurity and future cryptographic solutions.

RESULTS & DISCUSSION

Cryptography is a safe precaution to ensure secure communication (Sasikumar, 2024). Cryptography includes

symmetric-key cryptography, asymmetric-key cryptography, and Hash functions. Asymmetric-Key cryptography leverages a public key for encryption and a private key for decryption. Traditional asymmetric cryptography methods include those of RSA (Rivest Shamir Adleman) and ECC (Elliptic Curve Cryptography).

Elliptic Curve Cryptography (ECC)

Elliptic curve cryptography (ECC) is a public-key encryption method that utilizes elliptic curve hypotheses to generate cryptography keys that are faster, smaller, and more efficient. This is comparable to Rivest-Shamir-Adleman (RSA) and is widely employed in cryptocurrencies such as Ethereum and Bitcoin for digital signatures (Sasikumar, 2024). In ECC, both parties acquire publicly and privately a pair of keys that are used for enciphering & deciphering (Upreti, 2021). ECC employs an elliptic curve. A private key is a random number, while a public key is a point on the curve (Upreti, 2021).

Rivest-Shamir-Adleman (RSA)

Similar to ECC, the secure nature of RSA is solely because of the usage of large integers. In RSA, two prime numbers, larger than 512 bits, are taken and a series of advanced mathematical operations are carried out, resulting in the creation of two complex public keys, known to everyone, and two private keys, only known to the designer. The two large prime numbers are kept secret. The success of RSA lies in the fact that current algorithms are unable to factor the large integers used for the public and private keys into their prime components.

Shor's algorithm, proposed by Peter Shor in 1994, represents a groundbreaking development in the field of quantum computing (Hagar & Cuffaro, 2006). This algorithm efficiently factors large integers into their prime components exponentially faster than best-known classical algorithms. One of the implications of Shor's algorithm is its ability to break widely used public-key cryptography schemes, such as RSA (Zhu, 2001) and ECC. Shor's algorithm leverages quantum properties of superposition and entanglement to perform parallel computation. By doing so, it can efficiently find the prime factors of large numbers, a task that poses a significant challenge for classical computers (Ajala, 2024). As previously mentioned, RSA and ECC can ensure security simply because of the limitations of current algorithms to factor large integers into their prime components. Currently, there are no quantum computers able to run Shor's algorithm. However, because of properties of superposition and entanglement, quantum computers will easily be able to run advanced algorithms such as Shor's algorithm, being able to factor large integers into their prime components and rendering these traditional algorithms futile in a future where quantum computing is inevitable. Therefore, a new system of cryptography resistant to quantum computing will have to be adopted in the future.

Quantum computing represents a revolutionary step in computing, using complex concepts of quantum mechanics to solve problems that classical computers cannot solve. Central to this innovation involves qubits, the quantum equivalents of classical bits. Unlike classical bits, qubits leverage two

extraordinary phenomena: superposition and entanglement (Sood, 2024). Superposition is a fundamental principle of quantum mechanics where a quantum system exists in multiple states simultaneously. In classical computation, a bit is either 0 or 1, but a quantum bit (qubit) can be in a state of 0, 1, or any quantum superposition of these states (Youvan, 2024).

This property exponentially expands quantum computers' computational power, enabling them to process vast amounts of information simultaneously, allowing them to process advanced algorithms that traditional computers are incapable of processing. Entanglement is a quantum phenomenon where the states of two or more qubits become linked, such that the state of one qubit instantly influences the state of another, regardless of the distance between them. Entanglement is a phenomenon exclusive to quantum computers, giving them a huge advantage over classical computers. Entanglement allows for complex correlations between qubits that classical systems cannot replicate. This leads to greater efficiency and computational power. This interconnectedness is pivotal in applications such as QKD and PQC (Fatima, 2024). With the combined effect of superposition and entanglement, quantum computers are able to process and perform complex calculations that are simply not feasible for classical computers. This synergy of superposition and entanglement is what makes quantum computing so promising for tasks like cryptography, optimization, and simulating quantum systems.

As mentioned before, any development in the field of cryptography behaves like a double-edged sword, and therefore, developments in the field of quantum computing will have both positive and negative effects on traditional cryptography. Traditional methods like RSA and ECC are vulnerable to quantum algorithms such as Shor's Algorithm (Fatima, 2024). The ability of quantum computers to run such advanced algorithms will render traditional cryptography useless. Advanced solutions for the futurity of traditional cryptography algorithms in the future include quantum key distribution (QKD) and post-quantum cryptography (PQC). Post-quantum cryptography (PQC) and quantum cryptography. PQC concepts are based on a similar approach to classical algorithms: complex mathematical problems that cannot be solved in practical time by both classical and quantum computers (Dam, 2023). Quantum cryptography is based on the principles of quantum physics. Because the laws of quantum physics are unbreakable, the technology offers a long-term security solution. It is unaffected by advancements in computing or mathematics (Dervisevic, 2024). Therefore, the development of quantum cryptography is pivotal to ensuring the utmost security of data in a future where cyber threats will be able to utilize the exponentially greater computational power of quantum computers.

Quantum Key Distribution (QKD)

Quantum Key Distribution (QKD) (Bennet, 1984) is the most mature example of quantum technologies. It has been in experimental testing for over two decades and has only recently been used in commercial applications (Dervisevic, 2024). In contrast to conventional techniques that are prone to interception on public channels, QKD utilizes quantum

superposition and entanglement to facilitate a secure exchange of keys (Fatima, 2024). QKD requires two channels: a quantum channel and an authenticated public channel. These two channels are commonly referred to as a logical QKD link. Quantum transmission carried over the quantum channel cannot be passively monitored. When quantum carriers are monitored, they change state and, with high probability, reveal the presence of an eavesdropper (Dervisevic, 2024). Although theoretically secure, the characteristics of QKD that make it unique also create difficulties for its large-scale implementation. Implementation of QKD will require a physical connection between two users, making it a point-to-point technology (Dervisevic, 2024). Moreover, the properties of this kind of quantum transmission will prevent the usage of traditional technologies, limiting the range of technology, i.e., a technological revolution will be required for the implementation of QKD on a global scale, making QKD an impractical solution in today's time.

Post-Quantum Cryptography (PQC)

A crucial advancement in cybersecurity is post-quantum cryptography (PQC), which is motivated by the need to strengthen data security against the upcoming capabilities of quantum computers. In addition to multivariate, lattice, and code-based encryption, PQC includes a variety of techniques such as error-correcting codes and hash-based signatures (Fatima, 2024). Because of these unique properties, PQC will be far more advanced than current cryptography methods and will not demonstrate any vulnerabilities common to both RSA and ECC. However, the development and research of PQC is at a premature stage because of the absence of quantum computers capable of breaking RSA and ECC. Furthermore, there is no global standardization of PQC, and switching from RSA and ECC to PQC is currently unnecessary and poses various logistical challenges and technological constraints (Fatima, 2024).

Although PQC and QKD show promising results in providing security to digital systems against quantum computing, the field of quantum cryptography is premature and has no real urgency to aid development. Quantum computers are inevitable in the future, and therefore there will be a serious requirement for quantum-resistant cryptography such as PQC and QKD, which will have to be met with adequate development in quantum technologies to support their global standardization.

CONCLUSION

Through this research, the vulnerabilities of current cryptography methods such as RSA and ECC relative to the sheer power of quantum computers have been thoroughly investigated while exploring the requirements, limitations, and advantages of subsequent cryptography methods such as QKD in the quantum era. By analyzing how exactly current cryptography will lose importance due to the potential abilities of quantum computers, this research paper has emphasized the need for revolutionizing not only cryptography but also technology to support such quantum-resistant cryptography methods on a global scale. Although QKD and PQC show promising results in providing security in a future where quantum computing is inevitable, technological constraints

make these innovations impractical. Moving forward, research should prioritize creating technologies that can support the global standardization of PQC and QKD, scalable and viable cryptography protocols, overcoming the technological constraints demonstrated by QKD and PQC. Development in quantum computing should be supported by the development of quantum-resistant cryptography protocols and quantum technologies that can provide security in a future where quantum computers are inevitable. This development should be timely, as the maturity of quantum computing along with the prematurity of quantum-resistant cryptography protocols would result in the futility of current cryptography and a lack of digital security. Hence, international cooperation and timely research development with respect to the development of quantum technologies is of sincere importance to set a global standard for quantum computing and cryptography protocols as well as overcome technological constraints involved with quantum technology, ensuring robust encryption and digital security as society progresses towards the quantum era.

REFERENCES

1. Ajala, O. A., Okoye, C. C., & Daraojimba, A. (2024, February). Exploring and reviewing the potential of quantum computing in enhancing cybersecurity encryption methods. https://www.researchgate.net/publication/378522974_Exploring_and_reviewing_the_potential_of_quantum_computing_in_enhancing_cybersecurity_encryption_methods
2. Cherbal, S., Zier, A., Hebal, S., Louail, L., & Annane, B. (2023). Security in internet things: A review on approaches based on blockchain, machine learning, cryptography, and quantum computing. *The Journal of Supercomputing*, 80(3), 3738–3816. <https://doi.org/10.1007/s11227-023-05616-2>
3. Sihare, S. R. (2024). Quantum computing and cryptography in future computers. IGI Global.
4. Bavdekar, R., Chopde, E. J., Agrawal, A., Bhatia, A., & Tiwari, K. (2023, January). Post quantum cryptography: A review of techniques, challenges and standardizations. In 2023 International Conference on Information Networking (ICOIN) (pp. 146-151). IEEE.
5. Ahilan, A., & Jeyam, A. (2023). Breaking barriers in conventional cryptography by integrating with quantum key distribution. *Wireless Personal Communications*, 129(1), 549-567.
6. Sasikumar, K., & Nagarajan, S. (2024). Comprehensive review and analysis of cryptography techniques in cloud computing. *IEEE Access*, 12, 52325–52351. <https://doi.org/10.1109/access.2024.3385449>
7. Hagar, A., & Cuffaro, M. (2006). Quantum computing.
8. Zhu, H. (2001). Survey of computational assumptions used in cryptography broken or not by Shor's algorithm.
9. Sood, S. K. (2023). Quantum computing review: A decade of research. *IEEE Transactions on Engineering Management*, 71, 6662-6676.
10. Fatima, E., Aktar, A. N., & Arslan, M. (2024, September 1). Evaluating Quantum Cybersecurity: A Comparative Study of Advanced Encryption Methods. View of evaluating Quantum Cybersecurity: A comparative study of advanced encryption methods. <https://www.jcibi.org/index.php/Main/article/view/557/503>
11. Dervisevic, E., Tankovic, A., Fazel, E., Kompella, R., Fazio, P., Voznak, M., & Mehic, M. (2024). Quantum Key Distribution Networks--Key Management: A Survey. *arXiv preprint arXiv:2408.04580*.
12. Dam, D. T., Tran, T. H., Hoang, V. P., Pham, C. K., & Hoang, T. (2023). A survey of post-quantum cryptography: Start of a new race. *Cryptography*, 7(3), 40.
13. Azhari, R., & Salsabila, A. N. (2024). Analyzing the Impact of Quantum Computing on Current Encryption Techniques. *IAIC Transactions on Sustainable Digital Innovation (ITSDI)*, 5(2), 148-157.
14. Youvan, D. C. (2024). In-Flight Quantum Computation with Superposition and Entangled Steps: Transforming NP Complexity to O(1).